CLAIMS

1. An apparatus for performing cryptographic operations, comprising:

a cryptographic instruction, received by a computing device as part of an instruction flow executing on said computing device, wherein said cryptographic instruction prescribes one of the cryptographic operations;

translation logic, operatively coupled to said cryptographic instruction, configured to translate said cryptographic instruction into micro instructions, wherein said micro instructions are ordered to direct said computing device to load a second input text block and to execute said one of the cryptographic operations on said second input text block prior to directing said computing device to store an output text block corresponding to a first input text block;

whereby said output text block is stored during execution of said one of the cryptographic operations on said second input text block.

2. The apparatus as recited in claim 1, wherein said one of the cryptographic operations comprises:

an encryption operation, said encryption operation comprising encryption of a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks;

wherein said plurality of plaintext blocks comprise:

said first and second input text blocks; and

wherein said corresponding plurality of ciphertext blocks comprise:

said output text block.

3. The apparatus as recited in claim 1, wherein said one of the cryptographic operations comprises:

a decryption operation, said decryption operation comprising decryption of a plurality of ciphertext blocks to generate a corresponding plurality of plaintext blocks;

wherein said plurality of ciphertext blocks comprise:

said first and second input text blocks; and

wherein said corresponding plurality of plaintext blocks comprise:

said output text block.

4. The apparatus as recited in claim 1, further comprising:

execution logic, operatively coupled to receive said micro instructions, configured to store said output text block while executing said one of the cryptographic operations on said second input text block.

5. The apparatus as recited in claim 4, wherein said execution logic comprises a cryptography unit.

6. The apparatus as recited in claim 5, wherein said cryptography unit is configured to execute said one of the cryptographic operations according to the Advanced Encryption Standard (AES).

7. The apparatus as recited in claim 5, wherein said cryptography unit comprises:

a 2-stage round engine, configured to pipeline execution of said first and second input text blocks.

8. The apparatus as recited in claim 1, wherein said micro instructions comprise:

a load micro instruction, configured to direct said computing device to load said second input text block and to execute said one of the cryptographic operations on said second input text block; and

a store micro instruction, configured to direct said computing device to store said output text block.

9. The apparatus as recited in claim 1, wherein said cryptographic instruction is prescribed according to the x86 instruction format.

10. The apparatus as recited in claim 1, wherein said cryptographic instruction implicitly references a plurality of registers within said computing device.

11. The apparatus as recited in claim 10, wherein said plurality of registers comprises:

a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in memory for access of a plurality of input text blocks upon which said one of the cryptographic operations is to be accomplished, and wherein said plurality of input text blocks comprises said first and second input text blocks.

12. The apparatus as recited in claim 10, wherein said plurality of registers comprises:

a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding plurality of output text blocks, said corresponding plurality of output text blocks being generated as a result of accomplishing said one of the cryptographic operations upon a plurality of input text blocks, and wherein said plurality of output text blocks comprise said output text block.

13. The apparatus as recited in claim 10, wherein said plurality of registers comprises:

a third register, wherein contents of said third register indicate a number of text blocks within a plurality of input text blocks.

14. The apparatus as recited in claim 10, wherein said plurality of registers comprises:

a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in memory for access of cryptographic key data for use in accomplishing said one of the cryptographic operations.

15. The apparatus as recited in claim 10, wherein said plurality of registers comprises:

a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in memory, said fourth location comprising said initialization vector location, contents of said initialization vector location comprising an initialization vector or initialization vector equivalent for use in accomplishing said one of the cryptographic operations.

16. The apparatus as recited in claim 10, wherein said plurality of registers comprises:

a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in memory for access of a control word for use in accomplishing said one of the cryptographic operations, wherein said control word prescribes cryptographic parameters for said one of the cryptographic operations.

17. An apparatus for performing cryptographic operations, comprising:

translation logic, configured to translate a cryptographic instruction into a sequence of micro instructions, said sequence of micro instructions comprising:

a first micro instruction, directing that a second input text block be loaded and that one of the cryptographic operations be executed on said second input text block; and

a second micro instruction, directing that a first output text block be stored, said first output text block corresponding to a first input text block upon which said one of the cryptographic operations is executed;

wherein said translation logic issues said first micro instruction prior to issuing said second micro instruction;

whereby said output text block is stored during execution of said one of the cryptographic operations on said second input text block.

18. The apparatus as recited in claim 17, wherein said one of the cryptographic operations comprises:

an encryption operation, said encryption operation comprising encryption of a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks;

wherein said plurality of plaintext blocks comprise:

said first and second input text blocks; and wherein said corresponding plurality of ciphertext blocks comprise:

said output text block.

19. The apparatus as recited in claim 17, wherein said one of the cryptographic operations comprises:

a decryption operation, said decryption operation comprising decryption of a plurality of ciphertext blocks to generate a corresponding plurality of plaintext blocks;

wherein said plurality of ciphertext blocks comprise:

said first and second input text blocks; and

wherein said corresponding plurality of plaintext blocks comprise:

said output text block.

20. The apparatus as recited in claim 17, further comprising:

a cryptography unit, operatively coupled to receive said micro instructions, configured to store said output text block while executing said one of the cryptographic operations on said second input text block.

21. The apparatus as recited in claim 20, wherein said cryptography unit is configured to execute said one of the cryptographic operations according to the Advanced Encryption Standard (AES).

22. The apparatus as recited in claim 20, wherein said cryptography unit comprises:

a 2-stage round engine, configured to pipeline execution of said first and second input text blocks.

23. The apparatus as recited in claim 17, wherein said cryptographic instruction is prescribed according to the x86 instruction format.

24. A method for performing cryptographic operations in a device, the method comprising:

translating a cryptographic instruction that prescribes execution of one of the cryptographic operations into a first micro instruction and a second micro instruction, the first micro instruction directing the device to load a second input text block be loaded and to execute the one of the cryptographic operations on the second input text block, the second micro instruction directing the device to store a first output text block, where the first output text block correspond to a first input text block upon which said the of the cryptographic operations is executed; and issuing the first micro instruction to a cryptography unit prior to issuing the second micro instruction to the cryptography unit;

whereby said issuing causes the output text block to be stored during execution of the one of the cryptographic operations on the second input text block.

25. The method as recited in claim 24, wherein said translating comprises:

via the first micro instruction, prescribing that an encryption operation be executed on the second text block to generate a corresponding second ciphertext block.

26. The apparatus as recited in claim 24, wherein said translating comprises:

via the first micro instruction, prescribing that a decryption operation be executed on the second text block to generate a corresponding second plaintext block.

27. The apparatus as recited in claim 24, further comprising:

executing the first and second micro instructions within a cryptography unit, wherein said executing comprises:

storing the output text block while performing the one of the cryptographic operations on the second input text block.

28. The apparatus as recited in claim 24, wherein the cryptographic instruction prescribes execution of the one of the cryptographic operations according to the Advanced Encryption Standard (AES).

29. The apparatus as recited in claim 24, further comprising:

executing the first and second micro instructions within a cryptography unit, wherein said executing comprises pipelining the first and second input text blocks through a 2-stage round engine.